WHAT IS CLAIMED IS:

1. A method of accessing a storage area network (SAN), comprising:

retrieving a first value from a first copy of a password table;

using the first value to retrieve a second value from the first copy of the password table;

encrypting the first value according to a first copy of an encryption key;

sending the encrypted first value to a node of the SAN;

decrypting the encrypted first value according to a second copy of the encryption key;

using the decrypted first value to retrieve a third value from a second copy of the password table;

encrypting the third value according to the second copy of the encryption key and sending the encrypted third value back to a switch of the SAN;

decrypting the third value according to the first copy of the encryption key and comparing the decrypted third value with the second value; and

allowing access to the SAN if the third value and the second value match.

2. A method of claim 1, further comprising:

responsive to an event selected from a power on event and a software reset event, reading a serial identification corresponding to a host;

generating a code value based upon the serial number;

comparing the generated code value with a previously determined code value; and

denying access to the SAN if the generated code value and the previously determined code value differ.

3. The method of claim 2, wherein the code value is further based on a time stamp and date stamp.

4. The method of claim 1, wherein the SAN is a Fibre Channel compliant SAN.

5. The method of claim 1, further comprising, periodically executing a key generation application that generates a unique password table and encryption key for each node attached to the SAN.

6. The method of claim 5, wherein the key generation application requires privileged access.

7. The method of claim 5, wherein the password tables and encryption keys for each node are distributed to each node manually.

8. The method of claim 5, wherein the password tables and encryption keys for each node are distributed over an encrypted link.

9. A data processing network, comprising:

a switch port including controller, receiver, transmitter, non-volatile store, and memory, wherein the switch non-volatile storage includes a first copy of a password table and a first copy of an encryption key;

a node including processor, non-volatile storage, memory, and a host bus adapter, wherein the node non-volatile storage includes a second copy of the password table and a second copy of the encryption key; and

wherein the node memory contains at least of a portion of a node software interface and the switch memory contains at least a portion of a switch software interface, wherein the software interfaces contain instructions for retrieving a password from the first copy of the password table in response to a login request, using the password to determine a first response, sending the password to the node, using the password to determine a second response from the second copy of the password table, sending the second response back to the node, comparing the first and second responses; and denying the login request if the first and second response differ.

10. The network of claim 9, further comprising a key server application comprised of a set of instructions for generating the encryption key and the key password table for the node and switch.

11. The network of claim 10, wherein the key server application generates an encryption key and password table for each node-switch pair of the network.

12. The network of claim 10, wherein the encryption key and password table are stored on a portable storage device and manually distributed to the node.

13. The network of claim 10, wherein the encryption key and password table are distributed to the node via an external network.

14. The network of claim 10, wherein the key server application is executed periodically to generate new keys and passwords tables.

15. The network of claim 9, wherein the first and second copies of the password table are encrypted according to encryption key and wherein the software interfaces include instructions for encrypting and decrypting the responses and the passwords according to the encryption key.

16. The network of claim 9, wherein the node software interface further contains instructions for reading a serial identification corresponding to a host, generating a code value based upon the serial number, comparing the generated code value with a previously determined code value; and denying access to the SAN if the generated code value and the previously determined code value differ.

17. The network of claim 16, wherein the instructions for generating a code value are executed in response to an event selected from a power on event and a software reset.

18. The network of claim 9, wherein the switch comprises a Fibre Channel compliant switch.

19. A computer program product comprising a computer readable storage medium containing instructions for authorizing access to a storage area network, the instructions comprising:

a retriever enabled to retrieve a first value from a first copy of a password table;

means for using the retriever and the first value to retrieve a second value from the first copy of the password table;

an encryptor for encrypting the first value according to a first copy of an encryption key;

means for sending the encrypted first value to a node of the SAN;

a decryptor for decrypting the encrypted first value according to a second copy of the encryption key;

means for using the decrypted first value to retrieve a third value from a second copy of the password table;

means for encrypting the third value according to the second copy of the encryption key and sending the encrypted third value back to a switch of the SAN;

means for decrypting the third value according to the first copy of the encryption key and comparing the decrypted third value with the second value; and

means for allowing access to the SAN if the third value and the second value match.

20. The computer program product of claim 19, further comprising:

a reader enabled to determine a serial identification corresponding to a host in response to an detecting an event selected from a power on event and a software reset event;

a code value generator enabled to generate a code value based upon the serial number;

a comparator enable to compare the generated code value with a previously determined code value; and

means for denying access to the SAN if the generated code value and the previously determined code value differ.

21. The computer program product of claim 20, wherein the code value is further based on a time stamp and date stamp.

22. The computer program product of claim 19, further comprising, a key generation application that generates a unique password table and encryption key for each node attached to the SAN.